PRIME PUMAthematics

26 februari 2018

Oplossingen

1 It's a plot!

Verzameling die door PlotZer maar niet door PlotPar geplot kan worden:
Merk op dat elke niet-constante veelterm willekeurig grote (absolute) waarden bereikt. De enige begrensde deelverzamelingen van $\mathbb{R}^2$ die PlotPar kan plotten zijn dus singletons. PlotZer kan veel meer begrensde deelverzamelingen van $\mathbb{R}^2$ plotten, bijvoorbeeld:

- de eenheidscirkel (input $r(x,y) = x^2 + y^2 - 1$),
- een willekeurige eindige deelverzameling E van $\mathbb{R}^2$ (input $r(x,y) = \prod_{(a,b)\in E}((x-a)^2 + (y-b)^2)$).

Verzameling die door PlotPar maar niet door PlotZer geplot kan worden:
Een mogelijk voorbeeld wordt gegeven door de halfrechte $H = \{(x,x) : x \in \mathbb{R}_{\geqslant 0}\}$. Deze kan geplot worden door input $p(x) = x^2, q(x) = x^2$ in te voeren in PlotPar. Stel nu dat PlotZer H plot bij input $r(x,y)$. Beschouw de veelterm $d(x) = r(x,x)$. Uit het veronderstelde volgt dat elk positief reëel getal een nulpunt is van $d(x)$. De veelterm $d(x)$ is dus constant gelijk aan nul (indien niet-constant, zou d hoogstens evenveel nulpunten als zijn graad hebben). Maar dan plot het programma PlotZer bij input $r(x,y)$ ook punten (x,x) met x strikt negatief, wat in tegenstrijd is met het veronderstelde.

2 Een machtig jaar

Beschouw de getallen $m_i = \sum_{j=1}^{i} 2018^j$ voor $1 \leqslant i \leqslant 2018$. Wegens het duivenhokprincipe zijn er minstens twee van deze getallen m_{i_1} en m_{i_2} met $i_1 < i_2$ die tot dezelfde restklasse mod k behoren. $m_{i_2} - m_{i_1} = 2018^{i_1+1} + \cdots + 2018^{i_2}$ is dus deelbaar door k, $n_1 = i_1 + 1$ en $n_2 = i_2$ zijn dan de gezochte getallen.

3 Afleidingsmanoeuvre

(a) Zij $f \in V$, merk op dat uit de limiet in de opgave volgt dat

$$(\forall x \in \mathbb{R})(f(x) = 0 \vee f'(x) = 0). \qquad (*)$$

Beschouw de functie $g : \mathbb{R} \to \mathbb{R}$ bepaald door $g(x) = f(x)^2$ voor alle reële x. Omdat f afleidbaar is, is g dat ook, we vinden $g'(x) = 2f(x)f'(x) = 0$ op heel $\mathbb{R}$. Dit impliceert dat $g(x)$ maar één constante beeldwaarde $C \in \mathbb{R}_{\geqslant 0}$ bereikt. Dan kan f enkel de waarden $\{-\sqrt{C}, \sqrt{C}\}$ bereiken. Bereikt f echter twee verschillende waarden, dan zou f (continu) ook alle tussenliggende waarden bereiken en dus zeker een waarde die niet bevat is in $\{-\sqrt{C}, \sqrt{C}\}$. Dit is een tegenspraak. Er volgt dat f constant is en dan ook het te bewijzen.

(b) We bewijzen dat V enkel constante functies bevat. We werken hiervoor uit het ongerijmde: zij $f \in V$ niet-constant. Dan bestaat zeker een $a \in \mathbb{R}$ waarvoor $f(a) \neq 0$. Z.v.v.a. geldt $f(a) > 0$. Dan bestaat $r \in \mathbb{R}_{>0}$ zo dat f strikt positief is op het interval $]a - r, a + r[$.
Uit $(*)$ volgt dan $f'(x) = 0$ op het interval $]a - r, a + r[$ en bijgevolg is f constant gelijk aan $f(a)$ in dit interval. Beschouw nu de verzamelingen

$$\{x \in \mathbb{R}_{<a} : f(x) \neq f(a)\}, \{x \in \mathbb{R}_{>a} : f(x) \neq f(a)\}.$$

Omdat f niet-constant is, is ten minste een van beide niet leeg. Z.v.v.a. is dit de tweede verzameling. Beschouw dan

$$I := \inf\{x \in \mathbb{R}_{>a} : f(x) \neq f(a)\}.$$

Merk op dat $a + r \leqslant I$ en dus $a < I$.
Claim 1: $f(I) = f(a)$.
Inderdaad, indien $f(I) \neq f(a)$, dan zou f (continu) op het interval $]a, I[$ ook een waarde verschillend van $f(a)$ aannemen (bijvoorbeeld $\frac{f(a)+f(I)}{2}$), wat in tegenspraak zou zijn met de definitie van I.
Zij nu $\varepsilon \in \mathbb{R}_{>0}$ willekeurig. Uit de eigenschappen van infima volgt dat er een $j \in]I, I + \varepsilon[$ bestaat met $f(j) \neq f(a)$. Maar dan moet er in het interval $]I, j]$ een nulpunt van f bevat zijn, want anders zou $f'(x) = 0$ moeten gelden op dit interval, zodat f constant zou zijn op dit interval, waaruit zou volgen dat $f(a) = f(I) = f(j)$.
We hebben nu aangetoond dat I een ophopingspunt van nulpunten van f is. Door continuiteit is I dan ook een nulpunt van f. Dit is in tegenspraak met $f(I) = f(a) > 0$.

Opmerking:
Gebruik makend van enkele basisbegrippen uit de topologie, kunnen we als volgt een alternatieve oplossing voor puntje (b) neerschrijven.
Wegens $(*)$ geldt $f(x) \neq 0 \implies f$ afleidbaar in x en $f'(x) = 0$. Stel nu $f \in V$ en f niet-constant, en kies $a \in \mathbb{R}$ met $b := f(a) \neq 0$. Wegens continuïteit bestaat een open interval I rond a met $0 \notin f[I]$. Wegens voorgaande opmerking is f afleidbaar op I, $f' = 0$ op I, en dus $(\forall x \in I)(f(x) = b)$. Hieruit volgt dat $f^{-1}(b)$ open is. Wegens continuïteit is $f^{-1}(b)$ ook gesloten. Aangezien $\mathbb{R}$ samenhangend is en $a \in f^{-1}(b)$ is $f^{-1}(b) = \mathbb{R}$. Dit is strijdig, want f werd verondersteld niet-constant te zijn.

4 $\mathbf{Pu^+ + Ma^-}$

(a) Indien U involutief is, dan is $U - U^T \in \{A \in \mathbb{C}^{n\times n} : AU + U^T A = 0\}$. Indien U ook onvolutief is, moet dus ook noodzakelijk $U - U^T = 0$.

(b) Antwoord: De enige twee matrices die zowel involutief als onvolutief zijn, zijn I en $-I$.
We formuleren en bewijzen eerst volgend lemma.

Lemma. *Zij V een eindig dimensionale vectorruimte en $f : V \to V$ een lineaire afbeelding. Indien f een involutie is die verschilt van de identieke afbeelding, dan bestaat $v \in V \setminus \{0\}$ waarvoor $f(v) = -v$.*

Bewijs 1. Kies een basis $\mathcal{B}$ voor V. Zij M de matrixvoorstelling van f ten opzichte van $\mathcal{B}$. Dan geldt $M^2 = I$, wat te herschrijven valt tot $(M+I)(M-I) = 0$. Indien de matrix $M+I$ inverteerbaar is, dan volgt uit de vorige gelijkheid dat $M - I = 0$ en dus is f de identieke afbeelding. Indien de matrix $M + I$ singulier is heeft het stelsel $(M + I)v = 0$ een van nul verschillende oplossing. □

Bewijs 2. Indien f verschilt van de identieke afbeelding, kies dan $w \in V$ waarvoor $f(w) \neq w$. Beschouw $v := f(w) - w \neq 0$. Het is duidelijk dat $f(v) = -v$. □

Bewijs 3. Het minimaalpolynoom $p(x)$ van f is een deler van het polynoom $x^2 - 1$. Indien f verschilt van de identieke afbeelding, dan verschilt $p(x)$ van $x - 1$ en dus $p(x) \in \{x + 1, x^2 - 1\}$. In beide gevallen is -1 een wortel van $p(x)$ en dus een eigenwaarde van f. □

Zij U zowel involutief als onvolutief. Beschouw de vectorruimte V van complexe $n \times n$-matrices met de natuurlijke optelling en scalaire vermenigvuldiging. Beschouw de afbeelding $f : V \to V : A \mapsto U^T AU$. Het is duidelijk dat f lineair is en uit het involutief zijn van de matrix U volgt ook dat f een involutie is. Indien er een complexe $n \times n$-matrix A, verschillend van de nulmatrix, zou bestaan waarvoor $f(A) = U^T AU = -A$, dan zou volgen $AU + U^T A = 0$. Dit zou in tegenspraak zijn met onvolutief zijn van U. Uit het lemma volgt nu dat f gelijk is aan de identieke afbeelding, waaruit we meteen afleiden dat

$$U^T A = AU,$$

voor elke complexe $n \times n$-matrix A.
Zij $1 \leqslant k \neq l \leqslant n$. Kiezen we in bovenstaande gelijkheid de matrix A als $A_{ij} = \delta_{ik}\delta_{jk}$, dan vinden we $U_{kl} = (U^T A)_{lk} = (AU)_{lk} = 0$. De matrix U is dus een diagonaalmatrix. Kiezen we nu $A_{ij} = \delta_{il}\delta_{jk}$ in de gelijkheid, dan vinden we $U_{ll} = (U^T A)_{lk} = (AU)_{lk} = U_{kk}$. Er volgt $U = \lambda I$ en omdat U involutief is volgt $\lambda \in \{-1, 1\}$.

Alternatief

Uit het ongerijmde, stel dus dat U ionvolutief is en $U \neq \pm I$.

Uit het involutief zijn volgt dat voor elke eigenwaarde λ van U geldt dat $\lambda \in \{-1, 1\}$. Schrijf nu U in zijn Jordan-normaalvorm, met Jordan-blokken van de vorm

$$\begin{pmatrix} 1 & 1 & & \\ & 1 & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{pmatrix} \text{ of } \begin{pmatrix} -1 & 1 & & \\ & -1 & \ddots & \\ & & \ddots & 1 \\ & & & -1 \end{pmatrix}.$$

Uit $U^2 = I$ en

$$\begin{pmatrix} \pm 1 & 1 & & \\ & \pm 1 & \ddots & \\ & & \ddots & 1 \\ & & & \pm 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & \pm 2 & \cdots & \\ & 1 & \ddots & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

volgt dat elk Jordan-blok dimensie 1 heeft, en dus dat U diagonaliseerbaar is. Schrijf

$$Q^{-1}UQ = \begin{pmatrix} I_k & 0 \\ 0 & -I_{n-k} \end{pmatrix},$$

voor een zekere $Q \in \mathrm{GL}_n(\mathbb{C})$ en $0 \leqslant k \leqslant n$. Uit het feit dat $U \neq \pm I$ volgt dat $k > 0$ en $k < n$. Zij nu $C \in \mathbb{C}^{k\times(n-k)}$ en $D \in \mathbb{C}^{(n-k)\times k}$ willekeurig maar niet beiden 0, en stel

$$B := \begin{pmatrix} 0_k & C \\ D & 0_{n-k} \end{pmatrix}.$$

Dan hebben we

$$\begin{pmatrix} 0_k & C \\ D & 0_{n-k} \end{pmatrix}\begin{pmatrix} I_k & 0 \\ 0 & -I_{n-k} \end{pmatrix} + \begin{pmatrix} I_k & 0 \\ 0 & -I_{n-k} \end{pmatrix}\begin{pmatrix} 0_k & C \\ D & 0_{n-k} \end{pmatrix} = 0$$

$$\implies QBQ^{-1}Q\begin{pmatrix} I_k & 0 \\ 0 & -I_{n-k} \end{pmatrix}Q^{-1} + Q\begin{pmatrix} I_k & 0 \\ 0 & -I_{n-k} \end{pmatrix}Q^{-1}QBQ^{-1} = 0$$

$$\implies AU + UA = AU + U^T A = 0,$$

met $A := QBQ^{-1} \neq 0$. Dit is in strijd met het onvolutief zijn.

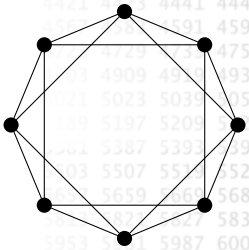
5 En garde!

Antwoord: Dit is mogelijk.

Oplossing 1
Nummer de musketiers met de getallen $\{0, \ldots, 7\}$. Laat musketier i schermen met musketier j als en slechts als het getal $i - j$ behoort tot een van de volgende restklassen modulo 8: $\{1 + 8\mathbb{Z}, 2 + 8\mathbb{Z}, 6 + 8\mathbb{Z}, 7 + 8\mathbb{Z}\}$. We controleren eenvoudig dat na afloop van deze duels aan de vereisten is voldaan. Inderdaad, volgende uitspraken gelden (optelling gebeurt modulo 8).

Musketiers a en $a + 1$ hebben beiden geschermd met musketier $a + 2$, maar geen van beiden heeft geschermd met musketier $a + 5$.
Musketiers a en $a + 2$ hebben beiden geschermd met musketier $a + 1$, maar geen van beiden heeft geschermd met musketier $a + 5$.
Musketiers a en $a + 3$ hebben beiden geschermd met musketier $a + 2$, maar geen van beiden heeft geschermd met musketier a.
Musketiers a en $a + 4$ hebben beiden geschermd met musketier $a + 2$, maar geen van beiden heeft geschermd met musketier a.

Oplossing 2
Om in te zien dat dit mogelijk is, volstaat het ook volgende graaf op 8 toppen te tekenen.



Dit levert precies dezelfde configuratie als deze beschreven in voorgaande oplossing.

6 PUMA-priemen

Lemma. *Een rij $(x_i)_i$ is p-nomenaal* $\iff$

$$\forall i \in \mathbb{N} : x_{i+p-3} \equiv x_i \mod p \text{ en } \forall k \in \{1, 2, \ldots, p-4\} : x_{i+k} \not\equiv x_i \mod p.$$

Bewijs. stel dat $(x_i)_i$ p-nomenaal is, dan is $p-3|p-3$, dus $x_{i+p-3} \equiv x_i \mod p$. Anderzijds geldt voor zulke k dat $p-3 \nmid k$, en dus $x_{i+k} \not\equiv x_i \mod p$. Voor de andere richting, schrijf $i-j = q(p-3)+r$ met $0 \leqslant r < p-3$. Dan geldt

$$p|x_i - x_j \iff x_{j+q(p-3)+r} \equiv x_j \mod p \iff x_{j+r} \equiv x_j \mod p$$
$$\iff r = 0 \iff p-3|i-j.$$

□

We zien dus dat een rij p-nomenaal is a. s. a. ze mod p periodiek is met periode $p-3$, en de eerste $p-3$ elementen over $p-3$ verschillende residuen mod p lopen.
Stel nu dat $X(n,m)$ p-nomenaal voor zekere p, n, m.

1. Herleiding naar een rij mod $\mathbf{p-1}$.
Als $p|n$, dan krijgen we mod p de nulrij, dus dit is uitgesloten. Voor $p \nmid n$ ziet men inductief in dat elk element van de geassocieerde rij niet nul is mod p. Nu is $(\mathbb{Z}/p\mathbb{Z})^\times$ cyclisch, en beschikt dus over een voortbrenger (primitieve wortel) g. Schrijf $n \equiv g^k$ en $x_i \equiv g^{y_i} \mod p$ voor zekere $k, y_i \in \{1, 2, \ldots, p-1\}$. Wegens de kleine stelling van Fermat is $n^p \equiv n \equiv g^k \mod p$ en $n^{m(p-2)} \equiv n^{-m} \equiv g^{-mk} \mod p$. Inductief vinden we voor de rij exponenten y_i:

$$(k, k+k, mk, mk+k, m^2k, m^2k+k, \ldots),$$

of $y_{2l} \equiv m^l k \mod p-1$ en $y_{2l+1} \equiv m^l k + k \mod p-1$. Wegens $g^a \equiv g^b \mod p \iff a \equiv b \mod p-1$, geldt er dat $X(n,m)$ p-nomenaal is a. s. a. de rij van exponenten $(y_i)_i$ periodiek is met periode $p-3$ en de eerste $p-3$ elementen over $p-3$ verschillende residuen mod $p-1$ lopen.

2. $(\mathbf{k}, \mathbf{p-1}) = \mathbf{1}$.
Aangezien elke y_i een veelvoud is van k en de eerste $p-3$ elementen onderling verschillend zijn, moet k inverteerbaar zijn mod $p-1$. Immers, als k niet inverteerbaar zou zijn mod $p-1$, dan zou het (additief) morfisme $(\mathbb{Z}/(p-1)\mathbb{Z}) \to (\mathbb{Z}/(p-1)\mathbb{Z}) : y \mapsto ky$ niet surjectief zijn en dus hoogstens $(p-1)/2$ waarden bereiken, wat strikt kleiner is dan $p-3$, tenzij $p=5$, maar dit geval zullen we later apart behandelen. Voor $p > 5$ is een nodige voorwaarde voor het p-nomenaal zijn van $X(n,m)$ dus dat $(k, p-1) = 1$.

3. $\mathbf{p = 2q + 1}$, $\mathbf{q}$ priem, $\mathbf{(m, p - 1) = 1}$ en $\mathbf{\mathrm{ord}_{p-1} m = (p - 3)/2 = q - 1}$.
Uit het feit dat de rij $(y_i)_i$ periodiek moet zijn met periode $p - 3$, halen we dat

$$m^{\frac{p-3}{2}} \equiv 1 \mod p-1 \quad \text{en} \quad \forall l \text{ met } 1 \leqslant l < \frac{p-3}{2} : m^l \not\equiv 1 \mod p-1.$$

Hieruit volgt dat m ook inverteerbaar mod $p-1$ moet zijn, en de orde van m mod $p-1$, $\mathrm{ord}_{p-1} m$, gelijk moet zijn aan $\frac{p-3}{2}$. Schrijf nu $p - 1 = 2^a q$ met $a > 0$ en q oneven. Met φ de Euler-totiënt functie hebben we

$$\mathrm{ord}_{p-1} m | \varphi(p-1) \implies 2^{a-1}q - 1 | 2^{a-1}\varphi(q).$$

Aangezien $\varphi(q) \leqslant q$ kan dit enkel indien $2^{a-1}\varphi(q) = 2^{a-1}q - 1$ (tenzij $q = 1$ en $a = 1$, maar dan is $p = 3$, en dat sluiten we uit). Hieruit volgt dat $a = 1$ en $\varphi(q) = q - 1$. De laatste gelijkheid impliceert dat q priem is, dus $p - 1 = 2q$ met q priem.

Samenvattend hebben we dat als $X(n, m)$ p-nomenaal is, dat dan $p = 2q + 1$ voor een priemgetal q, k en m inverteerbaar zijn mod $2q$ en $\mathrm{ord}_{2q} m = q - 1$.

We beweren dat ook het omgekeerde geldt: als $p = 2q + 1$ voor een priemgetal $q > 2$, dan is p een PUMA-priem. Zij h een voortbrenger van $(\mathbb{Z}/q\mathbb{Z})^\times$, en stel $m := h$ indien h oneven is, $m := h + q$ indien h even is. Wegens de Chinese Reststelling hebben we

$$m^l \equiv 1 \mod 2q \iff \begin{cases} m^l \equiv 1 \mod 2 \\ m^l \equiv 1 \mod q \end{cases} \iff h^l \equiv 1 \mod q,$$

zodat $\mathrm{ord}_{2q} m = q - 1$.
Bijgevolg is m een voortbrenger van $(\mathbb{Z}/2q\mathbb{Z})^\times = \{1, 3, \ldots, q-2, q+2, \ldots, 2q-1\}$. Kies nu k inverteerbaar mod $2q$, en stel $n := g^k \mod p$, waarbij g terug een primitieve wortel mod p is. Uit het feit dat m een primitieve wortel mod $2q$ is volgt dat $\{1, m, \ldots, m^{q-2}\}$ de verzameling van $q - 1$ inverteerbare residuen mod $2q$ is, en dus dat $\{1, 1+1, m, m+1, \ldots, m^{q-2}+1\}$ $2q-2$ verschillende residuen mod $2q$ vormen. Aangezien k inverteerbaar mod $2q$ is, is ook $\{k, k(1 + 1), km, k(m + 1), \ldots, k(m^{q-2} + 1)\}$ een verzameling van $2q - 2$ onderling verschillende residuen mod $2q$. De $p - 3 = 2q - 2$-periodiciteit volgt uit het feit dat $m^{q-1} \equiv 1 \mod 2q$. Bijgevolg is $X(n, m)$ een p-nomenale rij.

Ten slotte rekent men eenvoudig na dat voor het speciale geval $p = 5$, de keuzes $m = 1$ en $k = 1$ een p-nomenale rij opleveren. Voor de rij $(y_i)_i$ van exponenten mod $p - 1 = 4$ krijgt men dan:

$$1, 1 + 1 = 2, (2 + 3) \cdot 1 = 1, 2, \ldots.$$

De PUMA-priemen zijn dus precies de priemgetallen p van de vorm $p = 2q+1$, q priem.

Er zijn 25 priemgetallen q bevat in het interval $[1.5, 99.5]$, daarvan hebben er precies 10 de eigenschap dat ook $2q + 1$ priem is.
Er zijn dus precies 10 PUMA-priemen bevat in het interval $[4, 200]$.

Opmerking:
Priemgetallen q waarvoor ook $2q + 1$ priem is noemt men Sophie Germain primes, en de corresponderende priemgetallen $2q + 1$ (onze PUMA-priemen) safe primes. Men vermoedt dat er oneindig veel zulke priemgetallen bestaan, maar dit is nog niet bewezen.